

# **$b$ -SYMBOL DISTANCE DISTRIBUTION OF REPEATED-ROOT CYCLIC CODES**

HOJJAT MOSTAFANASAB AND ESRA SENGELEN SEVIM

**ABSTRACT.** Symbol-pair codes, introduced by Cassuto and Blaum [1], have been raised for symbol-pair read channels. This new idea is motivated by the limitations of the reading process in high-density data storage technologies. Yaakobi et al. [8] introduced codes for  $b$ -symbol read channels, where the read operation is performed as a consecutive sequence of  $b > 2$  symbols. In this paper, we come up with a method to compute the  $b$ -symbol-pair distance of two  $n$ -tuples, where  $n$  is a positive integer. Also, we deal with the  $b$ -symbol-pair distances of some kind of cyclic codes of length  $p^e$  over  $\mathbb{F}_{p^m}$ .

## 1. INTRODUCTION

Recently, it is possible to write information on storage devices with high resolution using advances in data storage systems. However, it causes a problem of the gap between write resolution and read resolution. Cassuto and Blaum [1, 2] laid out a framework for combating pair-errors, relating pair-error correction capability to a new metric called pair-distance. They proposed the model of symbol-pair read channels. Such channels are mainly motivated by magnetic-storage channels with high write resolution, due to physical limitations, each channel contains contributions from two adjacent symbols. Cassuto and List-syn [3] studied algebraic construction of cyclic symbol-pair codes. Yaakobi et al. [9] proposed efficient decoding algorithms for the cyclic symbol-pair codes. Chee et al. [5, 4] established a Singleton-type bound for symbol-pair codes and constructed codes that meet the Singleton-type bound. Hirotomo et al. [7] proposed the decoding algorithm for symbol-pair codes based on the newly defined parity-check matrix and syndromes.

For this new channels, the codes defined as usual over some discrete symbol alphabet, but whose reading from the channel is performed as overlapping pairs of symbols. Let  $\Xi$  be the alphabet consisting of  $q$  elements. Each element in  $\Xi$  is called a symbol. We use  $\Xi^n$  to denote the set of all  $n$ -tuples, where  $n$  is a positive integer. In the symbol-pair read channel, there are in fact two channels. If the stored information is  $x = (x_0, x_1, \dots, x_{n-1}) \in \Xi^n$ , then the symbol-pair read vector of  $x$  is

$$\pi(x) = [(x_0, x_1), (x_1, x_2), \dots, (x_{n-2}, x_{n-1}), (x_{n-1}, x_0)],$$

---

*Key words and phrases.*  $b$ -symbol-pair, distance distribution, cyclic codes.

and the goal is to correct a large number of the so called symbol-pair errors. The pair distance,  $d_p(x, y)$ , between two pair-read vectors  $x$  and  $y$  is the Hamming distance over the symbol-pair alphabet  $(\Xi \times \Xi)$  between their respective pair-read vectors, that is,  $d_p(x, y) = d_H(\pi(x), \pi(y))$ . The minimum pair distance of a code  $\mathcal{C}$  is defined as  $d_p(\mathcal{C}) = \min\{d_p(x, y) | x, y \in \mathcal{C} \text{ and } x \neq y\}$ . Accordingly, the pair weight of  $x$  is  $\omega_p(x) = \omega_H(\pi(x))$ . If  $\mathcal{C}$  is a linear code, then the minimum pair-distance of  $\mathcal{C}$  is the smallest pair-weight of nonzero code-words of  $\mathcal{C}$ . The minimum pair-distance is one of the important parameters of symbol-pair codes. This distance distribution is very difficult to compute in general, however, for the class of cyclic codes of length  $p^e$  over  $\mathbb{F}_{p^m}$ , their Hamming distance has been completely determined in [6]. In [10], Zhu et al. investigated the symbol-pair distances of cyclic codes of length  $p^e$  over  $\mathbb{F}_{p^m}$ .

For  $b \geq 3$ , the  $b$ -symbol read vector corresponding to the vector  $x = (x_0, x_1, \dots, x_{n-1}) \in \Xi^n$  is defined as

$$\pi_b(x) = [(x_0, x_1, \dots, x_{b-1}), (x_1, x_2, \dots, x_b), \dots, (x_{n-1}, x_0, \dots, x_{b-2})] \in (\Xi^b)^n.$$

We refer to the elements of  $\pi_b(x)$  as  $b$ -symbols. The  $b$ -symbol distance between  $x$  and  $y$ , denoted by  $d_b(x, y)$ , is defined as  $d_b(x, y) = d_H(\pi_b(x), \pi_b(y))$ . Similarly, we define the  $b$ -weight of the vector  $x$  as  $\omega_b(x) = \omega_H(\pi_b(x))$ . In the analogy of the definition of symbol-pair codes, the minimum  $b$ -symbol distance of  $\mathcal{C}$ ,  $d_b(\mathcal{C})$ , is given by  $d_b(\mathcal{C}) = \min\{d_b(x, y) | x, y \in \mathcal{C} \text{ and } x \neq y\}$ . For more information on these notions see [8].

We can rewrite [8, Proposition 9] for any arbitrary alphabet  $\Xi$ .

**Proposition 1.1.** *Let  $x \in \Xi^n$  be such that  $0 < \omega_H(x) \leq n - (b - 1)$ . Then*

$$\omega_H(\mathcal{C}) + b - 1 \leq \omega_b(\mathcal{C}) \leq b \cdot \omega_H(\mathcal{C}).$$

Referring to Proposition 1.1, we see that:

**Corollary 1.2.** *Let  $\mathcal{C}$  be a code. If  $0 < d_H(\mathcal{C}) \leq n - (b - 1)$ , then*

$$d_H(\mathcal{C}) + b - 1 \leq d_b(\mathcal{C}) \leq b \cdot d_H(\mathcal{C}).$$

In the next section we give a method to calculate the  $b$ -symbol distance of two  $n$ -tuples. We know that all cyclic codes of length  $p^e$  over a finite field of characteristic  $p$  are generated by a single “monomial” of the form  $(x - 1)^i$ , where  $0 \leq i \leq p^e$  (see [6]). Determining the  $b$ -symbol-pair distances of some kind of these cyclic codes is the main purpose of the next section.

## 2. MAIN RESULTS

In the following theorem we give a formula to calculate the  $b$ -symbol distance of two  $n$ -tuples.

**Theorem 2.1.** *Let  $x = (x_1, x_2, \dots, x_n)$  and  $y = (y_1, y_2, \dots, y_n)$  be two vectors in  $\Xi^n$  with  $0 < d_H(x, y) \leq n - (b - 1)$ . Suppose that*

$$A = \{1, 2, \dots, n\} \setminus \{r, r+1, r+2, \dots, s \mid r, s \text{ are such that } s-r \geq b-2 \text{ and } x_i = y_i \text{ for each } r \leq i \leq s \text{ and indices may wrap around modulo } n\},$$

and  $A = \cup_{l=1}^L B_l$  is a minimal partition of the set  $A$  to subsets of consecutive indices (every subset  $B_l = [s_l, e_l]$  is the sequence of all indices between  $s_l$  and  $e_l$ , inclusive, and is the smallest integer that achieves such partition, also indices may wrap around modulo  $n$ ). Then

$$d_b(x, y) = d_H(x, y) + e + L(b - 1),$$

where  $e = |\{i \mid i \in B_l \text{ for some } 1 \leq l \leq L \text{ such that } x_i = y_i\}|$ .

*Proof.* Since the partition is minimal, there are no two indices  $i, i + j$ , where  $j \in \{1, \dots, b - 1\}$ , that belong to different subsets  $B_l, B_{l'}$ . The  $b$ -symbol distance between  $x$  and  $y$  is equal to the sum of the sizes of the  $b$ -tuple subsets

$$\{(s_l - b + 1, s_l - b + 2, \dots, s_l), (s_l - b + 2, s_l - b + 3, \dots, s_l, s_l + 1), \dots, (s_l, s_l + 1, \dots, s_l + b - 1), \\ (s_l + 1, s_l + 2, \dots, s_l + b), \dots, (e_l, e_l + 1, \dots, e_l + b - 1)\}.$$

The number of  $b$ -tuples in each  $b$ -tuple subset equals  $|B_l| + b - 1$ , whence  $d_b(x, y) = \sum_{l=1}^L |B_l| + L(b - 1)$ . Furthermore, it is easy to see that  $\sum_{l=1}^L |B_l| = d_H(x, y) + e$  where  $e = |\{i \mid i \in B_l \text{ for some } 1 \leq l \leq L \text{ such that } x_i = y_i\}|$ .  $\square$

**Corollary 2.2.** Let  $x = (x_1, x_2, \dots, x_n) \in \Xi^n$  with  $0 < \omega_H(x) \leq n - (b - 1)$ . Suppose that

$$A = \{1, 2, \dots, n\} \setminus \{r, r+1, r+2, \dots, s \mid r, s \text{ are such that } s-r \geq b-2 \text{ and } x_i = 0\}$$

for each  $r \leq i \leq s$  and indices may wrap around modulo  $n$ ,

and  $A = \cup_{l=1}^L B_l$  is a minimal partition of the set  $A$  to subsets of consecutive indices (every subset  $B_l = [s_l, e_l]$  is the sequence of all indices between  $s_l$  and  $e_l$ , inclusive, and is the smallest integer that achieves such partition, also indices may wrap around modulo  $n$ ). Then  $\omega_b(x) = \omega_H(x) + e + L(b - 1)$ , where

$$e = |\{i \mid i \in B_l \text{ for some } 1 \leq l \leq L \text{ such that } x_i = 0\}|.$$

**Example 2.3.** Let  $n = 15$ ,  $b = 4$  and  $x = (0, 0, 1, 3, 0, 5, 0, 0, 0, 2, 0, 7, 0, 0, 0) \in \mathbb{Z}^{15}$ . We list all of the 4-tuples as follows:

$$(0, 0, 1, 3), (0, 1, 3, 0), (1, 3, 0, 5), (3, 0, 5, 0), (0, 5, 0, 0), (5, 0, 0, 0), (0, 0, 0, 2),$$

$$(0, 0, 2, 0), (0, 2, 0, 7), (2, 0, 7, 0), (0, 7, 0, 0), (7, 0, 0, 0), (0, 0, 0, 0), (0, 0, 0, 1).$$

Hence  $\omega_4(x) = 13$ . On the other hand,  $\omega_H(x) = 5$ ,  $e = 2$  and  $L = 2$ . Therefore, the equation  $\omega_b(x) = \omega_H(x) + e + L(b - 1)$  holds.

**Theorem 2.4.** ([6, Theorem 6.4]) Let  $\mathcal{C}$  be a cyclic code of length  $p^e$  over  $\mathbb{F}_{p^m}$ . Then  $\mathcal{C} = \langle (x - 1)^i \rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^e} - 1 \rangle}$ , for  $i \in \{0, 1, \dots, p^e\}$ . The Hamming distance  $d_H(\mathcal{C})$  is determined by

$$d_H(\mathcal{C}) = \begin{cases} 1 & \text{if } i = 0, \\ \beta + 2 & \text{if } \beta p^{e-1} + 1 \leq i \leq (\beta + 1)p^{e-1} \text{ where } 0 \leq \beta \leq p - 2, \\ (t + 1)p^k & \text{if } p^e - p^{e-k} + (t - 1)p^{e-k-1} + 1 \leq i \leq p^e - p^{e-k} + tp^{e-k-1}, \\ & \text{where } 1 \leq t \leq p - 1, \text{ and } 1 \leq k \leq e - 1, \\ 0 & \text{if } i = p^e. \end{cases}$$

From now on, in order to simplify the notation, for  $i \in \{0, 1, \dots, p^e\}$ , we denote each code  $\langle (x - 1)^i \rangle$  by  $\mathcal{C}_i$ .

**Proposition 2.5.** *If  $b \leq p^e$ , then  $d_b(\mathcal{C}_0) = b$ .*

*Proof.* By Theorem 2.4, we have that  $d_H(\mathcal{C}_0) = 1$ . So, by Corollary 1.2,  $b \geq d_b(\mathcal{C}_0) \geq d_H(\mathcal{C}_0) + b - 1 = b$ . Hence  $d_b(\mathcal{C}_0) = b$ .  $\square$

**Proposition 2.6.** *Let  $b < p^e$ . Then  $b+1 \leq d_b(\mathcal{C}_i) \leq 2b$  for every  $1 \leq i \leq p^{e-1}$ .*

*Proof.* By Theorem 2.4,  $d_H(\mathcal{C}_i) = 2$  for every  $1 \leq i \leq p^{e-1}$ . Hence,  $2b \geq d_b(\mathcal{C}_i) \geq 2 + (b-1) = b+1$ , by Corollary 1.2.  $\square$

Notice that, for two codes  $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_{p^m}^{p^e}$  with  $\mathcal{C} \subseteq \mathcal{C}'$ , we have  $d_b(\mathcal{C}) \geq d_b(\mathcal{C}')$ . We define  $d_b(\mathcal{C}_{p^e}) = 0$ .

**Proposition 2.7.** *Let  $b \leq p$  and  $e = 1$ . Then  $d_b(\mathcal{C}_i) = i + b$  for each  $0 \leq i \leq p - b$ .*

*Proof.* By Theorem 2.4,  $d_H(\mathcal{C}_i) = i + 1$  for  $0 \leq i \leq p - 1$ . Assume that  $0 \leq i \leq p - b$ . Hence, by Corollary 1.2,  $d_b(\mathcal{C}_i) \geq i + 1 + b - 1 = i + b$ . Moreover  $\omega_b((x-1)^i) = i + 1 + (b-1) = i + b$ . Then  $d_b(\mathcal{C}_i) = i + b$ .  $\square$

**Theorem 2.8.** *Let  $e \geq 2$  and  $1 \leq i \leq p^{e-1}$  such that  $i + b \leq p^e$  and  $i \leq b$ . Then  $d_b(\mathcal{C}_i) = i + b$ .*

*Proof.* Since  $i + b \leq p^e$ , then by Corollary 2.2,  $\omega_b((x-1)^i) = i + 1 + (b-1) = i + b$ . So,  $d_b(\mathcal{C}_i) \leq i + b$ . By Proposition 2.6,  $d_b(\mathcal{C}_i) \geq b + 1$ . Let  $c(x)$  be a polynomial in  $\mathbb{F}_{p^m}[x]$ . If  $\omega_b(c(x)) = j + b$  for some  $1 \leq j \leq i - 1$ , then  $i \leq b$  implies that  $c(x) = x^t(a_0 + a_1x + \dots + a_jx^j)$  where  $a_i$ 's are in  $\mathbb{F}_{p^m}$ ,  $a_0, a_j \neq 0$  and  $t$  is a non-negative integer. However  $c(x) \notin \mathcal{C}_i$ . So  $d_b(\mathcal{C}_i) = i + b$ .  $\square$

**Lemma 2.9.** *Let  $e$  and  $k$  be two integers such that  $e \geq 2$  and  $1 \leq k \leq e - 1$ . Suppose that  $c(x) = (x-1)^{p^e-p^{e-k}}g(x)$  where  $g(x)$  is a nonzero polynomial in  $\mathbb{F}_{p^m}[x]$  with  $d := \deg(g(x)) < p^{e-k}$  and  $b \leq p^e - d$ . Then*

- (1) *If  $d \leq p^{e-k} - b$  or  $g_k = 0$  for every  $0 \leq k \leq b - p^{e-k} + d - 1$ , then  $\omega_b(c(x)) = p^k \omega_b(g(x))$ .*
- (2) *If  $d > p^{e-k} - b$  and  $g_k \neq 0$  for some  $0 \leq k \leq b - p^{e-k} + d - 1$ , then  $\omega_b(c(x)) = p^k(\omega_b(g(x)) - (b-1) + \zeta)$  where  $\zeta = p^{e-k} - d - 1$ .*

*Proof.* Assume that  $g(x) = \sum_{j=0}^d g_j x^j$ . Thus

$$c(x) = \sum_{i=0}^{p^k-1} x^{ip^{e-k}} g(x) = \sum_{i=0}^{p^k-1} \sum_{j=0}^d g_j x^{ip^{e-k}+j}.$$

As usual, we identify the polynomial  $h(x) = h_0 + h_1x + \dots + h_nx^n$  with the  $p^k$ -time vector  $h = (h_0, h_1, \dots, h_n)$ . Therefore, we have  $c = (\widehat{g}, \dots, \widehat{g})$  where

$$\widehat{g} = (g_0, \dots, g_d, \overbrace{0, \dots, 0}^{(p^{e-k}-d-1)\text{-time}}).$$

We denote  $\omega_b(\widehat{g}(x)) := \omega_b(\widehat{g})$ . Since  $\pi_b(c) = \overbrace{[\pi_b(\widehat{g}), \dots, \pi_b(\widehat{g})]}^{p^k\text{-time}}$ , then  $\omega_b(c(x)) = p^k \omega_b(\widehat{g}(x))$ . On the other hand,  $\omega_b(g(x)) = \omega_b(g)$ , where

$$g = (g_0, g_1, \dots, g_d, \overbrace{0, \dots, 0}^{(p^e-d-1)\text{-time}}).$$

We can check that:

- (1) If  $d \leq p^{e-k} - b$  or  $g_k = 0$  for every  $0 \leq k \leq b - p^{e-k} + d - 1$ , then  $\omega_b(g) = \omega_b(\widehat{g})$ , i.e.,  $\omega_b(g(x)) = \omega_b(\widehat{g}(x))$ . Hence  $\omega_b(c(x)) = p^k \omega_b(g(x))$ .
- (2) If  $d > p^{e-k} - b$  and  $g_k \neq 0$  for some  $0 \leq k \leq b - p^{e-k} + d - 1$ , then  $\omega_b(g) = \omega_b(\widehat{g}) + (b-1) - \zeta$  where  $\zeta = p^{e-k} - d - 1$ , i.e.,  $\omega_b(g(x)) = \omega_b(\widehat{g}(x)) + (b-1) - \zeta$ . So,  $\omega_b(c(x)) = p^k(\omega_b(g(x)) - (b-1) + \zeta)$ .  $\square$

**Theorem 2.10.** *Let  $e$  and  $k$  be two integers such that  $e \geq 2$  and  $1 \leq k \leq e-1$ . If  $0 \leq i \leq p^{e-k-1}$  such that  $b+i \leq p^{e-k}$  and  $i \leq b$ , then  $d_b(\mathcal{C}_{p^e-p^{e-k}+i}) = p^k(b+i)$ .*

*Proof.* Fix  $0 \leq i \leq p^{e-k-1}$  such that  $b+i \leq p^{e-k}$  and  $i \leq b$ . Let  $0 \neq c(x) \in \mathcal{C}_{p^e-p^{e-k}+i}$ . Then, there exists  $0 \neq f(x) \in \mathbb{F}_{p^m}[x]$  such that  $c(x) = (x-1)^{p^e-p^{e-k}}(x-1)^i f(x)$ . Set  $g(x) := (x-1)^i f(x)$  and  $d := \deg(g(x))$ . Without loss of the generality we may assume that  $d < p^{e-k}$ . Notice that by Theorem 2.4,  $\omega_H(g(x)) \geq 2$ , and by Theorem 2.8,  $\omega_b(g(x)) \geq b+i$ . Regarding Lemma 2.9, we consider the following cases:

**Case 1.** If  $d \leq p^{e-k} - b$  or  $g_k = 0$  for every  $0 \leq k \leq b - p^{e-k} + d - 1$ , then  $\omega_b(c(x)) = p^k \omega_b(g(x)) \geq p^k(b+i)$ .

**Case 2.** If  $d > p^{e-k} - b$  and  $g_k \neq 0$  for some  $0 \leq k \leq b - p^{e-k} + d - 1$ , then  $\omega_b(c(x)) = p^k(\omega_b(g(x)) - (b-1) + \zeta)$  where  $\zeta = p^{e-k} - d - 1$ . If  $\omega_H(g(x)) \geq b+i$ , then Corollary 1.2 implies that  $\omega_b(g(x)) \geq b+i+b-1$ . Hence  $\omega_b(c(x)) \geq p^k(b+i+(b-1)-(b-1)) = p^k(b+i)$ . Assume that  $\omega_H(g(x)) = i+j$  for some  $2-i \leq j \leq b-1$ . It is easy to see that  $\omega_H(g(x)) + z = d+1$  where  $z = |\{l \mid 0 \leq l \leq d \text{ and } g_l = 0\}|$ . We claim that,  $z \geq b-j-\zeta$ . Otherwise  $d+1 < \omega_H(g(x)) + b-j-\zeta = i+j+b-j-(p^{e-k}-d-1) = i+b-p^{e-k}+d+1$ . But  $b+i \leq p^{e-k}$  leads us to a contradiction. Therefore the claim holds. So,  $\omega_b(g(x)) \geq i+j+b-j-\zeta+(b-1)$ . Thus  $\omega_b(c(x)) \geq p^k(\omega_b(g(x)) - (b-1) + \zeta) = p^k(i+b)$ . Hence  $d_b(\mathcal{C}_{p^e-p^{e-k}+i}) \geq p^k(i+b)$ . Moreover, by part (1) of Lemma 2.9,  $\omega_b((x-1)^{p^e-p^{e-k}+i}) = p^k \omega_b((x-1)^i) = p^k(b+i)$ . Consequently,  $d_b(\mathcal{C}_{p^e-p^{e-k}+i}) = p^k(b+i)$ .  $\square$

## REFERENCES

- [1] Y. Cassuto and M. Blaum. Codes for symbol-pair read channels. in Proc. IEEE Int. Symp. Inf. Theory, Austin, TX, USA, Jun, 988-992, 2010.
- [2] Y. Cassuto and M. Blaum. Codes for symbol-pair read channels. IEEE Trans. Inf. Theory, 57(12): 8011-8020, 2011.
- [3] Y. Cassuto and S. Litsyn. Symbol-pair codes: algebraic constructions and asymptotic bounds. in Proc. IEEE Int. Symp. Inf. Theory, St. Petersburg, Russia, Jul./Aug. 2348-2352, 2011.

- [4] Y. M. Chee, L. Ji and H. M. Kiah, C. Wang and J. Yin. Maximum distance separable codes for symbol-pair read channels. *IEEE Trans. Inf. Theory*, 59(11): 7259-7267, 2013.
- [5] Y. M. Chee, H. M. Kiah and C. Wang. Maximum distance separable symbol-pair codes. in *Proc. Int. Symp. Inf. Theory*, Cambridge, MA, USA, Jul. 2012, 2886-2890.
- [6] H. Q. Dinh. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. *Finite Fields Appl.*, 14(1): 22-40, 2008.
- [7] M. Hiroto, M. Takita and M. Morii. Syndrome decoding of symbol-pair codes. in *Proc. IEEE Inf. Theory Workshop*, Hobart, TAS, Australia, 162-166, 2014.
- [8] E. Yaakobi, J. Bruck and P. H. Siegel. Constructions and decoding of cyclic codes over  $b$ -symbol read channels. *IEEE Trans. Inf. Theory*, 62(4), 1541-1551, 2016.
- [9] E. Yaakobi, J. Bruck and P. H. Siegel. Decoding of cyclic codes over symbol-pair read channels. in *Proc. Int. Symp. Inf. Theory*, Cambridge, MA, USA, 2891-2895, 2012.
- [10] S. Zhu, Z. Sun and L. Wang. The symbol-pair distance distribution of repeated-root cyclic codes over  $\mathbb{F}_{p^m}$ . *arXiv: 1607.01887v1*, 2016.

Hojjat Mostafanasab

Department of Mathematics and Applications,

University of Mohaghegh Ardabili,

P. O. Box 179, Ardabil, Iran.

Email: h.mostafanasab@gmail.com, h.mostafanasab@uma.ac.ir

Esra Sengelen Sevim

Eski Silahtarağa Elektrik Santrali, Kazim Karabekir,

Istanbul Bilgi University,

Cad. No: 2/1334060, Eyüp Istanbul, Turkey.

Email: esra.sengelen@bilgi.edu.tr